Galois Categories

Swayam Chube

April 29, 2025

Contents

§1 Introduction

Let k be a field and fix a separable closure k_s of k and let $G_k := \mathrm{Gal}(k_s/k)$. If L is a finite separable extension of k, then there is a natural action of G_k on $\mathrm{Hom}_k(L, k_s)$ given by

$$G_k \times \mathrm{Hom}_k(k_s, L) \to \mathrm{Hom}_k(L, k_s) \qquad (g, \varphi) \mapsto g \circ \varphi.$$

It is straightforward to check that this is a continuous group action and $\mathrm{Hom}_k(L, k_s)$ is a transitive G_k-set.

Definition 1.1. A finite-dimensional k-algebra A is said to be *étale* over k if it is isomorphic to a finite direct product of separable extensions of k.

For an étale k-algebra A, there is a natural action

$$G_k \times \mathrm{Hom}_k(A, k_s) \to \mathrm{Hom}_k(A, k_s) \qquad (g, \varphi) \mapsto g \circ \varphi.$$

Theorem 1.2 (Fundamental Theorem of Galois Theory à la Grothendieck). The functor mapping a finite étale k-algebra A to the finite G_k-set $\mathrm{Hom}_k(A, k_s)$ gives an anti-equivalence between the category of finite étale k-algebras and finite (continuous) G_k-sets.

Proof. [Sza09, Theorem 1.5.4]. ■

Recall from basic algebraic topology that there is a similar "Galois correspondence" of covering spaces. Indeed, let X be a path connected, locally path connected, and semi-locally simply connected topological space and choose a base point $x_0 \in X$.

If $p : Y \to X$ is a finite-sheeted covering, then there is a natural action of $\pi_1(X, x_0)$ on the fibre $p^{-1}(x_0)$, known as the *monodromy action*. Since the fibre is finite, this action factors through a finite quotient of $\pi_1(X, x_0)$, thereby inducing a natural action of $\widehat{\pi_1(X, x_0)}$ on $p^{-1}(x_0)$.

Theorem 1.3 (Classification of Covering Spaces). The above functor sending a path connected covering space $p : Y \to X$ to the finite $\widehat{\pi_1(X, x_0)}$-set $p^{-1}(x_0)$ induces an equivalence of categories between the category of finite sheeted path connected covering spaces of X and the category of finite (continuous) $\widehat{\pi_1(X, x_0)}$-sets.

Proof. [Sza09, Corollary 2.3.9]. ■

Both the above results fit into the broad framework of "Galois categories" which this short essay attempts to explain. We shall mainly prove the fundamental theorem of Galois categories and be content with that. For further applications to the theory of schemes and the étale fundamental group, the reader is referred to [Len08].

§2 Preliminaries on Profinite Groups

Definition 2.1. A profinite group is an inverse limit of finite discrete topological groups. Note that a profinite group is always compact, Hausdorff, and totally disconnected.

Proposition 2.2. Let π be a profinite group acting on a set E. Then

(1) The action is continuous if and only if for each $e \in E$, $\operatorname{Stab}_\pi(e)$ is open in π.

(2) If E is finite, the action is continuous if and only if its kernel $\{\sigma \in \pi : \sigma e = e \ \forall\ e \in E\}$ is open in π.

(3) Any finite transitive π-set is isomorphic to π/π' for a certain open subgroup π' of π.

Proof. (1) If the action is continuous, then the function $\pi \to E$ given by $\sigma \mapsto \sigma e$ is continuous and the preimage of e, which is precisely the stabilizer of e in π, is open.

Conversely, suppose every stabilizer is open. Let $A : \pi \times E \to E$ denote the action. Since E is discrete, it suffices to show that $A^{-1}(e)$ is open for each $e \in E$. Let $e' \in \pi \cdot e$ and suppose $\tau_{e'} \in \pi$ is such that $\tau_{e'} e = e'$. Then

$$\{\sigma : \sigma e' = e\} = \tau_{e'}^{-1} \operatorname{Stab}_\pi(e'),$$

which is an open subset of π. Consequently,

$$A^{-1}(e) = \bigcup_{e' \in \pi \cdot e} \{(\sigma, e') : \sigma e' = e\} = \bigcup_{e' \in \pi \cdot e} \tau_{e'}^{-1} \operatorname{Stab}_\pi(e') \times \{e'\}$$

is an open subset of $\pi \times E$, as desired.

(2) The kernel of the action (denoted π') is the intersection of all the stabilizers. If E is finite, then since the stabilizers are open, the kernel is also open. Conversely, any open subgroup of π must have finite index, i.e., π' has finite index in π. Let $\tau_1, \dots, \tau_n$ be a collection of left coset representatives of π' in π, and supopse that for $1 \leqslant i \leqslant m$, we have $\tau_i e = e$, which implies

$$\pi_e = \bigcup_{i=1}^{m} \tau_i \pi',$$

and so the stabilizers of each $e \in E$ are open.

(3) This is trivial from (a) and (b). ■

§3 Galois Categories

§§ Statement of the Main Theorem

Definition 3.1. Let $\mathscr{C}$ be a category, X an object of $\mathscr{C}$, and G a subgroup of $\operatorname{Aut}_{\mathscr{C}}(X)$. The *quotient* of X by G is an object X/G of $\mathscr{C}$ together with a morphism $p : X \to X/G$ satisfying

(i) $p = p \circ \sigma$ for all $\sigma \in G$,

(ii) if $X \xrightarrow{f} Y$ is a morphism in $\mathscr{C}$ such that $f = f \circ \sigma$ for all $\sigma \in G$, then there is a unique morphism $X/G \xrightarrow{g} Y$ making

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, "p"'] & Y \\ X/G \arrow[ur, "g"'] & \end{tikzcd}$$

commute.

The quotient of an object by a group need not exist in a category, but when it does, it must be unique up to a unique isomorphism.

Definition 3.2. Let $\mathscr{C}$ be a category and $F : \mathscr{C} \to \mathbf{FinSets}$ a (covariant) functor from $\mathscr{C}$ to the category of finite sets. We say that the pair $(\mathscr{C}, F)$ is a *Galois category*, or that $\mathscr{C}$ is a Galois category with *fundamental functor* F, if the following axioms are satisfied:

(G1) There is a terminal object and $\mathscr{C}$ admits all fibred products.

(G2) An initial object exists in $\mathscr{C}$, finite coproducts exist in $\mathscr{C}$, and for any object in $\mathscr{C}$, the quotient by a finite group of automorphisms exists.

(G3) Any morphism u in $\mathscr{C}$ factors as $u = u' \circ u''$ where u' is a monomorphism and u'' is an epimorphism. Every monomorphism $X \xrightarrow{f} Y$ in $\mathscr{C}$ is an isomorphism of X with a direct summand of Y; i.e., there is an object $Z \xrightarrow{g} Y$ such that

$$\begin{tikzcd} & X \arrow[d, "f"] \\ Z \arrow[r, "g"'] & Y \end{tikzcd}$$

is a coproduct diagram.

(G4) The functor F sends terminal objects to terminal objects and commutes with fibred products.

(G5) The functor F sends initial objects to initial objects, commutes with finite coproducts, sends epimorphisms to epimorphisms, and commutes with passage to the quotient by a finite group of automorphisms.

(G6) If u is a morphism in $\mathscr{C}$ such that $F(u)$ is an isomorphism, then u is an isomorphism.

Proposition 3.3. Let $(\mathscr{C}, F)$ be a small Galois category and set $\mathscr{D} = [\mathscr{C}, \mathbf{FinSets}]$, the functor category between $\mathscr{C}$ and the category of finite sets. Then $\mathrm{Aut}_{\mathscr{D}}(F)$ is a profinite group acting continuously on $F(X)$ for every $X \in \mathscr{C}$.

Proof. An element of $\mathrm{Aut}_{\mathscr{D}}(F)$ is a natural isomorphism $\eta : F \Rightarrow F$, i.e, each $\eta_X : F(X) \to F(X)$ is an isomorphism. Hence, we can identify $\mathrm{Aut}_{\mathscr{D}}(F)$ with a subgroup of $\prod_{X \in \mathscr{C}} \mathfrak{S}_{F(X)}$, where $\mathfrak{S}_{F(X)}$ is the group of permutations of $F(X)$. In particular,

$$\mathrm{Aut}_{\mathscr{D}}(F) = \left\{ (\eta_X)_X \in \prod_{X \in \mathscr{C}} \mathfrak{S}_{F(X)} : \text{ for each } Y \xrightarrow{f} Z \text{ in } \mathscr{C},\ \eta_Z \circ F(f) = F(f) \circ \eta_Y \right\}.$$

Let $Y \xrightarrow{f} Z$ be a morphism in $\mathscr{C}$. Then the set

$$\mathfrak{A}_f = \left\{ (\eta_X)_X \in \prod_{X \in \mathscr{C}} \mathfrak{S}_{F(X)} : \eta_Z \circ F(f) = F(f) \circ \eta_Y \right\}.$$

is closed, as it is the finite union of the closed sets

$$\prod_{\substack{X \in \mathscr{C} \\ X \neq Y, Z}} \mathfrak{S}_{F(X)} \times \{\eta_Y\} \times \{\eta_Z\},$$

where $\eta_Y \in \mathfrak{S}_{F(Y)}$ and $\eta_Z \in \mathfrak{S}_{F(Z)}$ satisfy $\eta_Z \circ F(f) = F(f) \circ \eta_Y$. Now, since

$$\mathrm{Aut}_{\mathscr{D}}(F) = \bigcap_{\substack{Y \xrightarrow{f} Z \\ \text{in } \mathscr{C}}} \mathfrak{A}_f,$$

it is a closed subgroup of $\prod_{X \in \mathscr{C}} \mathfrak{S}_{F(X)}$, so that it is a profinite group.

Finally, the map $\mathrm{Aut}_{\mathscr{D}}(F) \times F(X) \to F(X)$ given by $((\eta_X)_{X \in \mathscr{C}}, a) \longmapsto \eta_X(a)$ defines an action of $\mathrm{Aut}_{\mathscr{D}}(F)$ on $F(X)$. The stabilizer of each $a \in F(X)$ is precisely

$$\mathrm{Aut}_{\mathscr{D}}(F) \times \left(\prod_{\substack{Y \in \mathscr{C} \\ Y \neq X}} \mathfrak{S}_{F(Y)} \times \mathrm{Stab}_{\mathfrak{S}_{F(X)}}(a) \right),$$

which is an open subgroup of $\mathrm{Aut}_{\mathscr{D}}(F)$. Due to Proposition 2.2, this action is continuous. ■

Interlude 3.4 (Construction of the Main Functor). Let $(\mathscr{C}, F)$ be a small Galois category. Define the functor $H : \mathscr{C} \to \mathrm{Aut}(F)$-**sets** sending each $X \in \mathscr{C}$ to $F(X)$ with the $\mathrm{Aut}(F)$-action as defined in the proof of Proposition 3.3. If $Y \xrightarrow{f} Z$ is a morphism in $\mathscr{C}$, then the induced morphism $F(f) : F(Y) \to F(Z)$ is $\mathrm{Aut}(F)$-linear: indeed, if $\eta = (\eta_X)_X \in \mathrm{Aut}(F)$, then for $y \in Y$,

$$F(f)\,(\eta y) = F(f)\,(\eta_Y y) = \eta_Z\,(F(f)(z)) = \eta F(f)(z).$$

Theorem 3.5 (Fundamental Theorem of Galois Categories). Let $(\mathscr{C}, F)$ be an essentially small Galois category. Then

(1) The functor $H : \mathscr{C} \to \mathrm{Aut}(F)$-**sets** is an equivalence of categories.

(2) If π is a profinite group such that the categories $\mathscr{C}$ and π-**sets** are equivalent by an equivalence, that when composed with the forgetful functor π-**sets** $\to$ **FinSets** yields the funtor F, then π is canonically isomorphic to $\mathrm{Aut}(F)$.

(3) If F' is a second fundamental functor on $\mathscr{C}$, then F and F' are naturally isomorphic.

(4) If π is a profinite group such that the categories $\mathscr{C}$ and π-**sets** are equivalent, then there is an isomorphism of profinite groups $\pi \cong \mathrm{Aut}(F)$ that is canonically determined up to an inner automorophism of $\mathrm{Aut}(F)$.

$\boxed{\text{Henceforth, let } (\mathscr{C}, F) \text{ be a small Galois category.}}$

§§ Subobjects and connected objects

Definition 3.6. Lt $X \in \mathscr{C}$. Consider the set $\{Y \to X \text{ a monomorphism}\}/\sim$ where

$$Y \xrightarrow{f} X \sim Y' \xrightarrow{f'} X$$

if and only if there is an isomorphism $Y \xrightarrow{\cong} Y'$ making

$$\begin{tikzcd} Y \arrow[r, "\cong"] \arrow[d, "f"'] & Y' \arrow[dl, "f'"] \\ X & \end{tikzcd}$$

commute. Every equivalence class in the above is called a *subobject* of X.

Lemma 3.7. f is a monomorphism if and only if $F(f)$ is injective.

Proof. Let $Y \xrightarrow{f} X$. We first show that f is a monomorphism if and only if the canonical map $p_1 : Y \times_X Y \to Y$ is an isomorphism. If f is a monomorphism, then it is clear that

$$\begin{tikzcd} Y \arrow[r, equal] \arrow[d, equal] & Y \arrow[d, "f"] \\ Y \arrow[r, "f"'] & X \end{tikzcd}$$

is a coproduct diagram, so that $p_1 : Y \times_X Y \to Y$ is an isomorphism.

Conversely, suppose $p_1 : Y \times_X Y \to Y$ is an isomorphism and consider the commutative diagram

$$\begin{tikzcd} Y \arrow[dr, dotted, "\theta"] \arrow[drr, bend left, "\mathbf{id}_Y"] \arrow[ddr, bend right, "\mathbf{id}_Y"'] & & \\ & Y \times_X Y \arrow[r, "p_1"] \arrow[d, "p_2"] & Y \arrow[d, "f"] \\ & Y \arrow[r, "f"'] & X \end{tikzcd}$$

Since p_1 is an isomorphism, it follows that $\theta = p_1^{-1}$ is an isomorphism. Further, since $p_2 \circ \theta = \mathbf{id}_Y$, we must have that $p_1 = p_2$.

Now, suppose $h_1, h_2 : Z \to Y$ are morphisms in $\mathscr{C}$ satisfying $f \circ h_1 = f \circ h_2$, then there is a morphism $\varphi : Z \to Y \times_X Y$ making the required diagram commute. But then

$$h_1 = p_1 \circ \varphi = p_2 \circ \varphi = h_2,$$

so that f is a monomorphism.

Coming back to the proof of the Lemma, we have

$$\begin{aligned} F(f) \text{ is injective } &\iff F(f) \text{ is a monomorphism} \\ &\iff F(p_1) \text{ is an isomorphism} \\ &\iff p_1 \text{ is an isomorphism} \\ &\iff f \text{ is a monomorphism,} \end{aligned}$$

where the first equivalence follows from the classification of monomorphisms in **FinSets**, the second and last equivalences follow from what we just proved and **(G4)**, and the third isomorphism follows from **(G6)**. ■

Lemma 3.8. Two monomorphisms $Y \xrightarrow{f} X$ and $Y' \xrightarrow{f'} X$ are representative of the same subobject of X if and only if $F(f)(F(Y)) = F(f')(F(Y'))$ as subsets of $F(X)$.

Proof. Suppose the two objects represent the same subobject of X. Then there is an isomorphism $\theta : Y \xrightarrow{\sim} Y'$ such that $f = f' \circ \theta$. Then, $F(f)(F(Y)) = F(f') \circ F(\theta)(F(Y))$ but $F(\theta)$ is an isomorphism, so is surjective and hence $F(f)(F(Y)) = F(f')(F(Y'))$.

Conversely, suppose $F(f)(F(Y)) = F(f')(F(Y'))$. As F commutes with fibred products, we have the following pullback squares

$$\begin{tikzcd} Y \times_X Y' \arrow[r, "p_1"] \arrow[d, "p_2"'] & Y \arrow[d, "f"] \\ Y' \arrow[r, "f'"'] & X \end{tikzcd} \qquad \begin{tikzcd} F\left(Y \times_X Y'\right) \arrow[r, "F(p_1)"] \arrow[d, "F(p_2)"'] & Y \arrow[d, "F(f)"] \\ Y' \arrow[r, "F(f')"'] & X \end{tikzcd}$$

Since the latter is a pullback square, we have

$$F\left(Y \times_X Y'\right) = \{(y, y') \in F(Y) \times F(Y') \colon F(f)(y) = F(f')(y')\}.$$

As $F(f)$ and $F(f')$ are injective with the same image in X, it is clear that both $F(p_1)$ and $F(p_2)$ must be bijections, consequently, due to **(G6)**, both p_1 and p_2 must be isomorphisms isomorphisms in $\mathscr{C}$. Finally, this gives $f = f' \circ (p_2 \circ p_1^{-1})$, as desired. ■

Definition 3.9. An object $X \in \mathscr{C}$ is said to be *connected* if it has exactly two subobjects, $0 \to X$ and $\mathbf{id}_X : X \to X$.

Proposition 3.10. Every object in $\mathscr{C} \neq 0$ is the coproduct of its connected subobjects.

Proof. Let X be a non-initial object in $\mathscr{C}$. We shall argue by induction on $\#F(X)$. If $\#F(X) = 1$, then X is connected, for if $Y \xrightarrow{f} X$ is a subobject, then $F(Y) \xrightarrow{F(f)} F(X)$ is injective, so that $F(Y) = \emptyset$ or $F(Y) = F(X)$. In the latter case, $F(f)$ is an isomorphism and hence, so is f; on the other hand, if $F(Y) = \emptyset$, then Y must be the initial object of $\mathscr{C}$[1]. Suppose now that $\#F(X) \geqslant 2$; since there is nothing to prove when X is connected, we may suppose that X is not connected. Then there is a subobject $Y \xrightarrow{q_1} X$ of X which is neither initial, nor an isomorphism. Due to **(G3)**, there is a morphism $Z \xrightarrow{q_2} X$ such that $X = Y \coprod Z$. This coproduct diagram transforms into a coproduct diagram in **FinSets**, so that $F(q_2)$ is injective, consequently due to Lemma 3.7, q_2 is a monomorphism. It follows that $Z \xrightarrow{q_2} X$ is another subobject of X. The inductive hypothesis applies and we can write X coproduct of *some* of its connected components. Since $\#F(X)$ is finite, it is clear that this is a finite coproduct.

It remains to show that X is the disjoint union of *each* of its connected subobjects. Suppose $X = \coprod_{i=1}^n X_i$ and Y a connected subobject of X. I shall treat $F(Y)$ and $F(X_i)$ as subsets of $F(X)$ for ease of notation. Since $F(X) = \coprod_i F(X_i)$, there is some index j such that $F(Y) \times_{F(X)} F(X_j) = F(Y) \cap F(X_j) \neq \emptyset$. As a result, $Y \times_X X_j$ is not the initial object of $\mathscr{C}$. Since $F(Y \times_X X_j) \to F(X_j)$ and $F(Y \times_X X_j) \to F(Y)$ are injective, due to Lemma 3.7, the maps $Y \times_X X_j \to X_j$ and $Y \times_X X_j \to Y$ must be monomorphisms, and hence, must be isomorphisms. It follows that X_j and Y are the same subobject of X. ∎

Lemma 3.11. $\mathscr{C}$ admits all equalizers.

Proof. Let $f, g : X \to Y$ be morphisms in $\mathscr{C}$. There are two fibred product diagrams

$$\begin{tikzcd}
X \times_Y X \arrow[r, "p_1"] \arrow[d, "p_2"'] & X \arrow[d, "f"] \\
X \arrow[r, "g"'] & Y
\end{tikzcd}
\qquad
\begin{tikzcd}
(X \times_Y X) \times_{X \times X} X \arrow[r] \arrow[d] & X \arrow[d, "\mathbf{id}_X \times \mathbf{id}_X"] \\
X \times_Y X \arrow[r, "p_1 \times p_2"'] & X \times X
\end{tikzcd}
\qquad
\begin{tikzcd}
X \times X \arrow[r, "\pi_1"] \arrow[d, "\pi_2"'] & X \\
X & X \arrow[l, "\mathbf{id}_X"] \arrow[u, "\mathbf{id}_X"'] \arrow[ul, dotted]
\end{tikzcd}$$

We claim that $W = (X \times_Y X) \times_{X \times X} X \to X$ is the equalizer of f and g. Clearly, we have the following equality of compositions:

$$\begin{aligned}
W \to X \xrightarrow{f} Y &= W \to X \xrightarrow{\mathbf{id}_X} X \xrightarrow{f} Y \\
&= W \to X \to X \times X \xrightarrow{\pi_1} X \xrightarrow{f} Y \\
&= W \to X \times_Y X \to X \times X \xrightarrow{\pi_1} X \xrightarrow{f} Y \\
&= W \to X \times_Y X \xrightarrow{p_1} X \xrightarrow{f} Y \\
&= W \to X \times_Y X \xrightarrow{p_2} X \xrightarrow{g} Y \\
&= W \to X \times_Y X \to X \times X \xrightarrow{\pi_2} X \xrightarrow{g} Y \\
&= W \to X \to X \times X \xrightarrow{\pi_2} X \xrightarrow{g} Y \\
&= W \to X \xrightarrow{\mathbf{id}_X} X \xrightarrow{g} Y \\
&= W \to X \xrightarrow{g} Y.
\end{aligned}$$

If $h : Z \to X$ is such that $f \circ h = g \circ h$, then there is a unique map $\theta : Z \to X \times_Y X$ induced by $Z \xrightarrow{h} X$, which then induces a unique map $\phi : Z \to W$, as desired. ∎

Proposition 3.12. Let A be a connected object in $\mathscr{C}$ and $a \in F(A)$. Then for every $X \in \mathscr{C}$, the map

$$\mathscr{C}(A, X) \longrightarrow F(X) \qquad f \longmapsto F(f)(a)$$

is injective.

[1]Indeed, if 0 is "the" initial object of $\mathscr{C}$, then there is a unique morphism $0 \xrightarrow{u} Y$ in $\mathscr{C}$. But since $F(u)$ is an isomorphism in **FinSets**, it follows from **(G6)** that u is an isomorphism.

Proof. Let $f, g \in \mathscr{C}(A, X)$ be such that $F(f)(a) = F(g)(a)$, and let (C, θ) be the equalizer of f, g, which is known to exist due to Lemma 3.11. Since F commutes with fibred products, it must commute with equalizers too, hence $(F(C), F(\theta))$ is an equalizer of $F(f), F(g) : F(A) \to F(X)$. In particular, $F(\theta)$ is injective, so that θ is a monomorphism due to Lemma 3.7. Moreover,

$$a \in F(C) = \{b \in F(A) \colon F(f)(b) = F(g)(b)\} \neq \emptyset,$$

and hence C is not the initial object of $\mathscr{C}$, whence $\theta : C \to A$ is an isomorphism, which implies $f = g$. ■

Interlude 3.13. Consider the set $I = \{(A, a) \colon A \text{ connected},\ a \in F(A)\} / \sim$ where $\sim$ is the equivalence relation:

$$(A, a) \sim (B, b) \iff \exists\ f : A \to B \text{ an isomorphism such that } F(f)(a) = b.$$

We can define a partial order on I by

$$(A, a) \geqq (B, b) \iff \exists\ f : A \to B \text{ a morphism such that } F(f)(a) = b.$$

Note that due to Proposition 3.12 the above map f, if it exists, is unique. We claim that $(I, \geqq)$ is a directed set under this order relation:

Reflexivity: Taking $f = \mathbf{id}_A$, we have $F(\mathbf{id}_A)(a) = a$, so $(A, a) \geqq (A, a)$.

Anti-symmetry: If $(A, a) \geqq (B, b)$ and $(B, b) \geqq (A, a)$, then there are morphisms $A \xrightarrow{f} B$ and $B \xrightarrow{g} A$ such that $F(f)(a) = b$ and $F(g)(b) = a$. Consequently, $F(g \circ f)(a) = a$ and $F(f \circ g)(b) = b$. Using Proposition 3.12, it follows that $g \circ f = \mathbf{id}_A$ and $f \circ g = \mathbf{id}_B$, that is, $(A, a) = (B, b)$.

Transitivity: If $(A, a) \geqq (B, b) \geqq (C, c)$ and $A \xrightarrow{f} B$ and $B \xrightarrow{g} C$ are the corresponding maps, then $g \circ f : A \to C$ is such that

$$F(g \circ f)(a) = F(g) \circ F(f)(a) = F(g)(b) = c.$$

Directedness: Let $(A, a), (B, b) \in I$. Choose a connected subobject $C \to A \times B$ such that the image of $F(C)$ in $F(A \times B) = F(A) \times F(B)$ contains $a \times b$; further, let $c \in C$ be the unique element in $F(C)$ mapping to $a \times b$. Compose the monomorphism $C \to A \times B$ with the canonical projections $A \times B \xrightarrow{p_1} A$ and $A \times B \xrightarrow{p_2} B$ to obtain maps f_1 and f_2. Then it is clear that $F(f_1)(c) = a$ and $F(f_2)(c) = b$, so that $(C, c) \geqq (A, a), (B, b)$.

We shall write $(A, a) \geqq_f (B, b)$ if we want to specify the morphism $A \xrightarrow{f} B$ satisfying $F(f)(a) = b$.

If $(A, a) \geqq_f (B, b)$, then the morphism $f : A \to B$ induces a natural transformation of functors $\mathscr{C}(B, -) \xrightarrow{- \circ f} \mathscr{C}(A, -)$. This gives us a projective system of functors in the functor category $[\mathscr{C}, \mathbf{FinSets}]$.

Theorem 3.14. There is an isomorphism of functors

$$\varinjlim_{(A,a) \in I} \mathscr{C}(A, -) \longrightarrow F(-) \qquad f \longmapsto F(f)(a)$$

Proof. Consider the maps $\phi_{(A,a)} : \mathscr{C}(A, X) \to F(X)$ given by $f \mapsto F(f)(a)$. If $(A, a) \geqq_\psi (B, b)$, then it is clear that the diagram

$$\begin{tikzcd} \mathscr{C}(A, X) \arrow[dr, "\phi_{(A,a)}"'] & & \mathscr{C}(B, X) \arrow[ll, "- \circ \psi"'] \arrow[dl, "\phi_{(B,b)}"] \\ & X & \end{tikzcd}$$

commutes. This clearly induces a map $\phi : \varinjlim_{(A,a) \in I} \mathscr{C}(A, X) \to F(X)$ given by

$$\phi(f) = \phi_{(A,a)}(f) \quad \text{ if } f \in \mathscr{C}(A, X).$$

It suffices to show that this map is a bijection of sets, since then it would follow that ϕ is an isomorphism of functors.

First, we show injectivity. Suppose $F(f)(a) = F(g)(b)$ for some $(A, a), (B, b) \in I$ and $f \in \mathscr{C}(A, X)$ and $g \in \mathscr{C}(B, X)$. Let $C \to A \times B$ be a connected subobject such that $(a, b) \in f(C)$, and let p_1', p_2' be the compositions of the projection maps $p_1 : A \times B \to A$ and $p_2 : A \times B \to B$ with the monomorphism $C \to A \times B$. It is then clear that $(C, c) \geqq (A, a)$ and $(C, c) \geqq (B, b)$.

Under the map $\mathscr{C}(A, X) \to \mathscr{C}(C, X)$, the morphism f maps to $f \circ p_1'$ and under the map $\mathscr{C}(B, X) \to \mathscr{C}(C, X)$, the morphism g maps to $g \circ p_2'$. We contend that these two maps are the same. Indeed, since $F(fp_1')(c) = F(gp_2')(c)$, due to Proposition 3.12, $fp_1' = gp_2'$. This shows that f and g are equal in $\varinjlim_{(A,a)\in I} \mathscr{C}(A, X)$.

Finally, to see surjectivity, take $x \in F(X)$ and consider $f : A \to X$, the connected component of X such that $x \in F(A)$. Then $(A, x) \in I$ and $F(f)(x) = x$. This completes the proof. ■

§§ Galois Objects

If A is a connected object, then we have the inequalities:

$$\# \operatorname{Aut}_{\mathscr{C}}(A) \leqslant \# \mathscr{C}(A, A) \leqslant \# F(A),$$

where the second inequality follows from Proposition 3.12. In particular, the set of automorphisms of A is finite, and therefore, it makes sense to talk about the quotient of a connected object by its group of automorphisms.

Definition 3.15. An object $A \in \mathscr{C}$ is called a *Galois object* if $A/\operatorname{Aut}_{\mathscr{C}}(A)$ is a terminal object.

Proposition 3.16. Let $X \in \mathscr{C}$. There exists $(A, a) \in I$ with A Galois such that the map $\mathscr{C}(A, X) \to F(X)$ given by $f \mapsto F(f)(a)$ is bijective.

Proof. Let $Y = X^{\#F(X)}$ be the product of $\#F(X)$ copies of X. As F commutes with products, we have $F(Y) = F(X)^{\#F(X)}$. Let us index the coordinates of Y by the elements of $F(X)$, and let $a \in F(Y)$ be the element having in the x-th coordinate the element $x \in F(X)$. Let A be the connected component of Y suc tthat $a \in F(A)$ and $f_x : A \to Y \to X$ be the composition of the monomorphism $A \to Y$ and the projectio on the x-th coordinate $p_x : Y \to X$. Then $f_x \in \mathscr{C}(A, X)$ and $F(f_x)(a) = x$. As a has all the elements of $F(X)$ in its coordinates, then as f_x varies, we obtain all the elements $x \in F(X)$, and so the map is bijective (since we already know about injectivity from Proposition 3.12).

Moreover, we have also obtained that the only morphisms in $\mathscr{C}(A, X)$ are the ones of the form f_x for a certain $x \in f(X)$. We contend that A is Galois. Let $a' \in F(A)$, $a' \neq a$. The map $\mathscr{C}(A, X) \to F(X)$ given by $f \mapsto F(f)(a')$ is bijective as it is injective and we have just seen that the two sets cardinality. As for all $g \in \mathscr{C}(A, X)$, $g = f_x$ for a certain x, this proves that a' has all the elements of $F(X)$ in its coordinates.

We shall show that there is an automorphism of Y sending a to a'. Let $a = (a_x)_{x\in F(X)}$ and $a' = (a_{\sigma(x)})_{x\in F(X)}$ where σ is a permutation of the set $F(X)$. Note that $\mathscr{C}(Y, Y) = \prod_{x\in F(X)} \mathscr{C}(Y, X)$ and consider the map $f = \prod_{x\in F(X)} p_{\sigma(x)}$. Then $F(f)(a) = \prod_{x\in F(X)} F(p_{\sigma(x)})(a) = (a_{\sigma(x)})_{x\in F(X)} = a'$. Taking the inverse permutation to σ we see that f is an isomorphism. Then the map $A \to Y \xrightarrow{\sigma} Y$ is a monomorphism, which induces an automorphism $A \xrightarrow{\tau} A'$ from A to another connected component A' of Y. Moreover, as $a' \in F(A) \cap F(A')$, and A, A' are connected, we must have $F(A) = F(A')$, so that $A = A'$ and therefore τ is an automorphism of A which sends a to a'. In conclusion $\operatorname{Aut}_{\mathscr{C}}(A)$ acts transitively on $F(A)$, and therefore A is Galois. ■

Remark 3.17. The above result shows that the subset $J \subseteq I$ corresponding to connected Galois objects is a cofinal subset of I, so

$$\varinjlim_{J} \mathscr{C}(A, -) \cong \varinjlim_{I} \mathscr{C}(A, -) \cong F.$$

§§ Construction of the Equivalence

Lemma 3.18. Let A be a connected Galois object, and B a connected object such that $\mathscr{C}(A, B) \neq \emptyset$. Then, the action

$$\operatorname{Aut}_{\mathscr{C}}(A) \times \mathscr{C}(, B) \to \mathscr{C}(A, B) \qquad (\sigma, f) \mapsto f \circ \sigma$$

is transitive.

Proof. Let $f \in \mathscr{C}(A, B)$, then we can factor $f = gh$ where h is an epimorphism and g is a monomorphism. Since B is connected, g must be an isomorphism since both A and B are connected. In particular, this means that $F(f)$ is an isomorphism. Thus, given $f' : A \to B$, there exists an $a' \in F(A)$ such that $F(f)(a') = F(f')(a)$. Since A is Galois, there exists a unique $\sigma \in \mathrm{Aut}_{\mathscr{C}}(A)$ such that $F(\sigma)(a) = a'$. Then $F(f\sigma)(a) = F(f')(a)$, and due to Proposition 3.12, we have that $f \circ \sigma = f'$. ■

Lemma 3.19. Let $(A, a), (B, b) \in J$, $(A, a) \geqq_f (B, b)$. Given $\sigma \in \mathrm{Aut}_{\mathscr{C}}(A)$, there exists a unique $\tau \in \mathrm{Aut}_{\mathscr{C}}(B)$ such that $\tau \circ f = f \circ \sigma$ and the mapping $\sigma \mapsto \tau$ is a surjective group homomorphism $\mathrm{Aut}_{\mathscr{C}}(A) \to \mathrm{Aut}_{\mathscr{C}}(B)$.

Proof. Let $a' := F(\sigma)(a)$ and $b' := F(f)(a')$. Then, since B is Galois, there exists a unique $\tau \in \mathrm{Aut}_{\mathscr{C}}(B)$ such that $F(\tau)(b) = b'$ due to Proposition 3.16. So, we have

$$F(f\sigma)(a) = b' = F(\tau f)(a) \implies f \circ \sigma = \tau \circ f$$

due to Proposition 3.12. It remains to show that such a $\tau \in \mathrm{Aut}_{\mathscr{C}}(B)$ is unique. Indeed, if there were two automorphisms $\tau_1, \tau_2 \in \mathrm{Aut}_{\mathscr{C}}(B)$ satisfying the property, i.e., $\tau_1 \circ f = f \circ \sigma = \tau_2 \circ f$, then $F(\tau_1)(b) = F(\tau_2)(b)$. Due to Proposition 3.12, it follows that $\tau_1 = \tau_2$.

Finally, we must show that the association $\sigma \mapsto \tau$ is a surjective group homomorphism $\mathrm{Aut}_{\mathscr{C}}(A) \to \mathrm{Aut}_{\mathscr{C}}(B)$. Indeed, if $\sigma_1 \mapsto \tau_1$ and $\sigma_2 \mapsto \tau_2$, then we have

$$f\sigma_1\sigma_2 = \tau_1 f \sigma_2 = \tau_1\tau_2 f,$$

and so $\sigma_1\sigma_2 \mapsto \tau_1\tau_2$. This proves that the association $\sigma \mapsto \tau$ is a group homomorphism. Further, due to Lemma 3.18, the action of $\mathrm{Aut}_{\mathscr{C}}(A)$ on $\mathscr{C}(A, B)$ is transitive, and hence, given $\tau \in \mathrm{Aut}_{\mathscr{C}}(B)$, there exists a $\sigma \in \mathrm{Aut}_{\mathscr{C}}(A)$ such that $\tau \circ f = f \circ \sigma$, whence the association $\sigma \mapsto \tau$ is surjective, thereby completing the proof. ■

Note that the above result gives rise to an inverse system indexed by J. Set

$$\pi := \varprojlim_J \mathrm{Aut}_{\mathscr{C}}(A) \subseteq \prod_J \mathrm{Aut}_{\mathscr{C}}(A).$$

Proposition 3.20. For all $X \in \mathscr{C}$, the action

$$\varprojlim_J \mathrm{Aut}_{\mathscr{C}}(A) \times \varinjlim_J \mathscr{C}(A, X) \longrightarrow \varinjlim_J \mathscr{C}(A, X) \qquad ((\sigma_A)_{A\in J}, f) \longmapsto f \circ \sigma^{-1}$$

defines a functor $H' : \mathscr{C} \to \pi$-**sets**.

Proof. First, we must check that this action is well-defined. Let $f_A \in \mathscr{C}(A, X)$ and $f_B \in \mathscr{C}(B, X)$ be representatives of the same element in $\varinjlim_J \mathscr{C}(A, X)$. This means that there exists a $(C, c) \in J$ such that $(C, c) \geqq_{f_1} (A, a)$ and $(C, c) \geqq_{f_2} (B, b)$ and $f_B \circ f_2 = f_C = f_A \circ f_1$. Let $(\sigma_A)_{A\in J} \in \varprojlim_J \mathrm{Aut}_{\mathscr{C}}(A)$. Then we have

$$f_A f_1 \sigma_C^{-1} = f_C \sigma_C^{-1} = f_B f_2 \sigma_C^{-1}.$$

But $\sigma_A^{-1} f_1 = f_1 \sigma_C^{-1}$ and $\sigma_B^{-1} f_2 = f_2 \sigma_C^{-1}$. Therefore,

$$f_C \sigma_C^{-1} = f_A \sigma_A^{-1} f_1 = f_B \sigma_B^{-1} f_2,$$

whence $f_A \sigma_A^{-1} = f_B \sigma_B^{-1}$ in $\varinjlim_B \mathscr{C}(A, X)$.

It is easy to check that the above action is continuous. We shall show functoriality. Let $f : X \to Y$ be a morphism in $\mathscr{C}$, then $H'(f)$ maps $(f_A)_{A\in J}$ to $(f \circ f_A)_{A\in J}$. Then it is clear that H' preserves compositions and maps the identity to the identity. ■

Remark 3.21. We have defined a functor $H' : \mathscr{C} \to \pi$-**sets** by endowing the functor $\varinjlim_J \mathscr{C}(A, -) \cong F(-)$. This isomorphism of functors induces a π-action on $F(X)$ for each $X \in \mathscr{C}$, which induces a functor $\mathscr{C} \to \pi$-**sets**, which, upon composing with the forgetful functor π-**sets** $\to$ **Sets** recovers F. All that remains is to show that H' is an equivalence of categories.

Proposition 3.22. Let B be a connected object in $\mathscr{C}$. Then $B \cong A/G$ for some Galois object A and G a finite subgroup of $\mathrm{Aut}_{\mathscr{C}}(A)$.

Proof. Due to Proposition 3.16 there exists a Galois object A and $a \in F(A)$ such that the map

$$\mathscr{C}(A, B) \longrightarrow F(B) \qquad f \longmapsto F(f)(a)$$

is bijective. But since $F(B) \cong \varinjlim_J \mathscr{C}(A, B)$ and $\mathrm{Aut}_{\mathscr{C}}(A)$ acts transitively on $\mathscr{C}(A, B)$, we have that $\mathrm{Aut}_{\mathscr{C}}(A)$ acts transitively on $H'(B)$, and therefore, $H'(B) \cong \mathrm{Aut}_{\mathscr{C}}(A)/G$, where G is the stabilizer of a certain element $f \in H'(B)$.

In particular, we have $\#F(B) = \#\,\mathrm{Aut}_{\mathscr{C}}(A)/G$. Further, for each $\sigma \in G$, we have $f \circ \sigma = \sigma$, consequently, there is a morphism $g : A/G \to B$ induced by f. Since $F(f)$ is surjective, so is $F(g)$. Moreover, $\#F(A/G) = \#F(A)/G = \#\,\mathrm{Aut}_{\mathscr{C}}(A)/G$, so that $F(g)$ is an isomorphism. It follows from **(G6)** that $B \cong A/G$, as desired. ∎

Proposition 3.23. The functor H' maps connected objects to connected objects.

Proof. For every connected object B, choose a Galois object A such that $\mathscr{C}(A, B) \cong F(B)$. Then $\mathrm{Aut}_{\mathscr{C}}(A)$ acts transitively on $\mathscr{C}(A, B)$. Further, since the maps in the inverse system $(\mathrm{Aut}_{\mathscr{C}}(A))_{A \in J}$ are surjective, it follows that π acts transitively on $H'(B)$, so that $H'(B)$ is a connected object in the category π-**sets**. ∎

Lemma 3.24. Let $f : X \to Z$ be an epimorphism in $\mathscr{C}$ and $g : W \to Z$ a non-trivial subobject. Then $W \times_Z X \to Z$ is a non-trivial subobject. In particular, if $X \to Z$ is an epimorphism and X is connected, then Z is connected.

Proof. First, we show that the map $p_2 : W \times_Z X \to X$ is a monomorphism. Indeed, let $s, t : Y \to W \times_Z X$ satisfy $p_2 s = p_2 t$.

$$\begin{tikzcd}
Y \arrow[dr, dotted] \arrow[drr, "p_1 s = p_1 t"] \arrow[ddr, "p_2 s = p_2 t"'] & & \\
& W \times_Z X \arrow[r, "p_1"] \arrow[d, "p_2"] & W \arrow[d, "g"] \\
& X \arrow[r, "f"'] & Z
\end{tikzcd}$$

Composing with f, we have $fp_2 s = fp_2 t$, and hence $gp_1 s = gp_2 t$. As g is a monomorphism, this implies that $p_1 s = p_1 t$. Thus $s, t : Y \to W \times_Z X$ makes the above diagram commute. Hence, $s = t$ by uniqueness. This proves that p_2 is a monomorphism.

It remains to check that it is a non-trivial subobject. For this, it is enough to check that $F(W \times_Z X)$ is neither the empty set, nor all of $F(X)$. Note that

$$F(W \times_Z X) = F(W) \times_{F(Z)} F(X) = \{(a, b) \in F(W) \times F(X) \colon F(f)(b) = F(g)(a)\}.$$

- If $F(W \times_Z X) = F(X)$, then since f is an epimorphism, this means that for all $z \in F(Z)$, there exists a pair $(a, b) \in F(W) \times F(X)$ such that $F(f)(b) = z$, and $F(g)(a) = z$, so that $F(g)$ is surjective. Since $F(g)$ is also injective, it must be an isomorphism, whence, due to **(G6)**, so is g, i.e., $W \to Z$ is the full subobject, a contradiction.
- If $F(W \times_Z X) = 0$, then there is no pair $(a, b) \in F(W) \times F(X)$ satisfying $F(g)(a) = F(f)(b)$. But as f is an epimorphism, we must have that $F(W) = 0$, so that W is the initial object in $\mathscr{C}$, a contradiction. ∎

Lemma 3.25. If $f, g : X \to Y$ are two morphisms in $\mathscr{C}$ satisfying $F(f) = F(g)$, then $f = g$.

Proof. Let $E \to X$ denote the equalizer of (f, g). As we have seen earlier, $F(E) \to F(X)$ is the equalizer of $(F(f), F(g))$. But since $F(f) = F(g)$, we must have that $F(E) \to F(X)$ is an isomorphism, whence due to **(G6)**, $E \to X$ is an isomorphism, so that $f = g$, as desired. ∎

Theorem 3.26. The functor $H' : \mathscr{C} \to \pi$-**sets** is an equivalence of categories.

Proof. It suffices to show that H' is fully-faithful and essentially surjective. Any π-set is a disjoint union of transitive orbits, so it suffices to show that every transitive π-set is of the form $H'(X)$ for some $X \in \mathscr{C}$ (this is because H' preserves coproducts).

Note that every trasitiv eπ-set is of the form $\mathrm{Aut}_{\mathscr{C}}(A)/G$ for some $G \subseteq \mathrm{Aut}_{\mathscr{C}}(A)$ and A connected Galois. Note that the map

$$\mathrm{Aut}_{\mathscr{C}}(A) \longrightarrow H'(A) \qquad f \longmapsto F(f)(a)$$

is bijective. Therefore the map

$$H'(A) \longrightarrow \mathrm{Aut}_{\mathscr{C}}(A) \qquad F(f)(a) \longmapsto f^{-1}$$

is a bijection, and $F(f\sigma^{-1}) \longmapsto \sigma f^{-1}$, so the map respects the π-action, and it is therefore an isomorphism of π-sets. Thus

$$H'(A/G) \cong H'(A)/G \cong \mathrm{Aut}_{\mathscr{C}}(A)/G,$$

thereby proving essential surjectivity.

As for fully-faithfulness, we already know that $\mathscr{C}(X,Y) \to \pi\text{-}\mathbf{sets}\,(H'(X), H'(Y))$ is injective due to Proposition 3.12. Therefore it would suffice to show that the sets have the same cardinality. First, we reduce this to the case of connected objects.

- For all $X \in \mathscr{C}$, wecan write a decomposition $X = \coprod_{i=1}^n X_i$, and due to the universal property of coproducts, we have
$$\mathscr{C}(X,Y) \cong \prod_{i=1}^n \mathscr{C}(X_i, Y).$$
As H' commutes with finite coproducts, we also have that
$$\pi\text{-}\mathbf{sets}(H'(X), H'(Y)) \cong \prod_{i=1}^n \pi\text{-}\mathbf{sets}\left(H'(X_i), H'(Y)\right),$$
whence we can reduce to the case that X is connected.

- Let $X \to Y$ be a morphism. Using **(G3)**, we can factor it as $X \xrightarrow{\text{epi}} Z \xrightarrow{\text{mono}} Y$. If X is connected, due to Lemma 3.24, we know that Z is connected too, and hence $Z \to Y$ is a connected component of Y. This shows that any morphism $X \to Y$ factors through connected components of Y, so that
$$\mathscr{C}(X,Y) \cong \coprod_{i=1}^n \mathscr{C}(X, Y_i)$$
for X connected. Using that H' maps connected components to connected components, we also have that
$$\pi\text{-}\mathbf{sets}\left(H'(X), H'(Y)\right) \cong \coprod_{i=1}^n \pi\text{-}\mathbf{sets}\left(H'(X), H'(Y_i)\right).$$

Now choose $A \in \mathscr{C}$ so that $X \cong A/G_1$ and $Y \cong A/G_2$. This can always be done: For example, one can take A a connected component of $X^{\#F(X)} \times Y^{\#F(Y)}$ and repeat the same proof of Proposition 3.16, and then use Proposition 3.22.

Then we have that $H'(X) \cong \mathrm{Aut}_{\mathscr{C}}(A)/G_1$ and $H'(Y) \cong \mathrm{Aut}_{\mathscr{C}}(A)/G_2$. Consider a morphism of π-sets, $f : \mathrm{Aut}_{\mathscr{C}}(A)/G_1 \to \mathrm{Aut}_{\mathscr{C}}(A)/G_2$. Then, $f(\tau G_1) = \tau\sigma G_2$, for a certain σ that completely characterizes f. The morphism is well-defined $\iff$ two representatives of the same class are mapped to the same element $\iff$ for all $g \in G_1$, $gG_1 \mapsto \sigma G_2 \iff$ for all $g \in G_1$, $g\sigma G_2 = \sigma G_2 \iff$ for all $g \in G_1$, $g\sigma \in \sigma G_2 \iff G_1\sigma \subseteq \sigma G_2$. Then

$$\#\pi\text{-}\mathbf{sets}\left(H'(X), H'(Y)\right) = \#\left\{\sigma G_2 \colon G_1\sigma \subseteq \sigma G_2\right\}.$$

On the other hand, the choice of A implies that $\mathrm{Aut}_{\mathscr{C}}(A)$ acts transitively on both $\mathscr{C}(A,X)$ and $\mathscr{C}(A,Y)$. Then, cosnider the projection morphisms $A \xrightarrow{h_1} A/G_1$ and $A \xrightarrow{h_2} A/G_2$. Given $f : X \to Y$, there exists a $\sigma \in \mathrm{Aut}_{\mathscr{C}}(A)$ such that $h_2\sigma = fh_1$.

$$\begin{tikzcd}
A \arrow[r, "h_1"] \arrow[d, "\sigma"'] & A/G_1 = X \arrow[d, "f"] \\
A \arrow[r, "h_2"'] & A/G_2 = Y
\end{tikzcd}$$

Note that $h_2\sigma = h_2\sigma' \iff \sigma'\sigma^{-1} \in G_2 \iff G_2 sigma = G_2\sigma'$, so f uniquely determines the coset $G_2\sigma$. Reciprocially, an element $\sigma \in \mathrm{Aut}_{\mathscr{C}}(A)$ gives rise to a morphism $f : X \to Y$ ifa nd only if $h_2\sigma$ factors through A/G_1, that is, if and only if $h_2\sigma\tau = h_2\sigma$, for all $\tau \in G_1$ if and only if $\sigma G_2 \subseteq G_2\sigma$. This proves that

$$\#\mathscr{C}(X, Y) = \#\{G_2\sigma \colon \sigma G_2 \subseteq G_2\sigma\}.$$

In conclusion, $\#\mathscr{C}(X, Y) = \#\pi\text{-}\mathbf{sets}(H'(X), H'(Y))$, thereby completing the proof. ■

§§ Proof of the Main Theorem

Lemma 3.27. Let π be a profinite group, $F : \pi\text{-}\mathbf{sets} \to \mathbf{Sets}$ the forgetful functor. Then $\mathrm{Aut}(F) \cong \pi$.

Proof. Note that given $\theta \in \mathrm{Aut}(F)$, the action of θ on every π-set is determined by its action on the transitive π-sets, and as every transitive π-set is isomorphic to one of the form π/π', with π' an open subgroup of π, the action of θ is totally determined by the action on the sets of this form.

Moreover, we know that in a compact totally disconnected group, every neighborhood of 1 contains an open normal subgroup. Therefore, there exists π'' an open normal subgroup of π such that $\pi'' \subseteq \pi'$. Consider the natural morphism of π-sets $f : \pi/\pi'' \twoheadrightarrow \pi/\pi'$. The automorphism θ of F has to commute with f. Let $\sigma \in \pi$ be such that $\theta_{\pi/\pi''}(\tau\pi'') = \tau\sigma\pi''$. Then we have $f \circ \theta_{\pi/\pi''}(\tau\pi'') = \tau\sigma\pi'$, and so $\theta_{\pi/\pi'} \circ f(\tau\pi') = \tau\sigma\pi'$. As $f(\tau\pi'') = \tau\pi'$, we have then $\sigma_{\pi/\pi'}(\tau\pi') = \tau\sigma\pi'$. Thus, the action of $\theta \in \mathrm{Aut}(F)$ is totally determined by the morphisms $\theta_{\pi/\pi'}$ where π' runs over open (and hence, finite index) normal subgroups of π.

Let π' be an open normal subgroup of π. Note that $\pi\text{-}\mathbf{sets}(\pi/\pi') \cong \pi/\pi'$, with the following isomorphism

$$\mathrm{Aut}_{\pi\text{-}\mathbf{sets}}(\pi/\pi') \to \pi/\pi' \qquad f \mapsto \tau^{-1}\pi' \text{ if } f(\pi') = \tau\pi'.$$

Now let $f : \pi/\pi' \to \pi/\pi$ be a set theoretic map commuting with all π-set automorphisms. Then $f(\tau\pi')\sigma = f(\tau\pi'\sigma)$ if and only if $f(\pi'\tau)\sigma = f(\pi'\tau\sigma)$. Let $f(\pi') = a\pi'$. Then $f(\pi'\sigma) = f(\sigma\pi') = f(\pi')\sigma = a\pi'\sigma$, so f is given by left multiplication by an element of π/π'. Therefore, we can define a map $\psi : \pi \to \mathrm{Aut}(F)$ given by

$$\psi(\sigma)_{\pi/\pi'}(\pi') = \sigma\pi'$$

for every open normal subgroup of π. We shall now show that this is an isomorphism of groups.

Well-defined: To see that $\psi(\sigma) \in \mathrm{Aut}(F)$, it is enough to check that it commutes with every morphism of π-sets, and this can clearly be reduced to proving that it commutes with every morphism $\pi/\pi' \to \pi/\pi''$, where π' and π'' are open normal subgroups of π. Let $f : \pi/\pi' \to \pi/\pi''$ be given by $f(\pi') = a\pi''$. Let $x \in \pi' \setminus \pi''$. Then $xa\pi''f(x\pi') = f(\pi') = a\pi''$ and hence $x\pi''a = \pi''a$ for all $x \in \pi'$. This implies $\pi'' \supseteq \pi'$, and it is clear that $\psi(\sigma)$ commutes with f, so ψ is well-defined.

Injectivity: This is clear because an element $\theta \in \mathrm{Aut}(F)$ is totally characterized by the coordinates $\theta_{\pi/\pi'} \in \pi/\pi'$, and

$$\pi \cong \varprojlim_{\pi' \text{ open normal}} \pi/\pi'.$$

Surjective: The fact that every morphism $\pi/\pi' \to \pi/\pi'$ commuting with π-set automorphisms is given by left product by an element of π/π' implies that every element of $\mathrm{Aut}(F)$ ha to be defined by left product by an element of $\varprojlim \pi/\pi' \cong \pi$.

This completes the proof. ■

Proof of Theorem 3.5. (b) Let π be a profinite group, and $H : \mathscr{C} \to \pi$-**sets** an equivalence that composed with the forgetful functor $F_1 : \pi$-**sets** $\to$ **Sets** yields F. Then we have $\mathrm{Aut}(F_1) \cong \pi$ by Lemma 3.27. Therefore, it would be enough to check that $\mathrm{Aut}(F) \cong \mathrm{Aut}(F_1)$.

Note that an automorphism $\varepsilon \in \mathrm{Aut}(F_1)$ induces naturally an automorphism of F, $\psi(\varepsilon) = \left(\varepsilon_{H(X)}\right)_{X \in \mathscr{C}}$. Indeed, for $A, B \in \pi$-**sets** and $f : A \to B$, there is a commutative diagram

$$\begin{tikzcd} F_1(A) \arrow[r, "F_1(g)"] \arrow[d, "\varepsilon_A"'] & F_1(B) \arrow[d, "\varepsilon_B"] \\ F_1(A) \arrow[r, "F_1(g)"'] & F_1(B) \end{tikzcd}$$

Given $Y, Z \in \mathscr{C}$ and $f : Y \to X$, we can take $A = H(X)$, $B = H(Y)$, and $g = H(f)$ and substituting into the diagram above, taking into account that $F_1 \circ H = F$, it yields

$$\begin{tikzcd} F(Y) \arrow[r, "F(f)"] \arrow[d, "\varepsilon_{H(Y)}"'] & F(Z) \arrow[d, "\varepsilon_{H(Z)}"] \\ F(Y) \arrow[r, "F(f)"'] & F(Z) \end{tikzcd}$$

Reciprocially, we shall show that every automorphism of F will induce an automorphism of F_1. As H is an equivalence of categories, we have that there exists a functor $G : \pi$-**sets** $\to \mathscr{C}$, and an isomorphism of functors $\theta : \mathbf{id} \Rightarrow HG$:

$$\begin{tikzcd} A \arrow[r, "g"] \arrow[d, "\theta_A"'] & B \arrow[d, "\theta_B"] \\ HG(A) \arrow[r, "HG(g)"'] & HG(B) \end{tikzcd}$$

Then let $\sigma \in \mathrm{Aut}(F)$, and take $Y = G(A)$, $Z = G(B)$, $f = G(g)$. We have commutative diagrams:

$$\begin{tikzcd} F(Y) \arrow[r, "F(f)"] \arrow[d, "\sigma_Y"'] & F(Z) \\ F(Y) \arrow[r, "F(f)"'] & F(Z) \end{tikzcd} \qquad \begin{tikzcd} F_1HG(A) \arrow[r, "F_1HG(g)"] \arrow[d, "\theta_{G(A)}"'] & F_1HG(B) \arrow[d, "\theta_{G(B)}"] \\ F_1HG(A) \arrow[r, "F_1HG(g)"'] & F_1HG(B) \end{tikzcd}$$

Then, we can define $\varphi(\sigma) := (\varphi(\sigma)_A)_{A \in \pi\text{-}\mathbf{sets}} = \left(F_1(\theta_A^{-1})\sigma_{G(A)}F_1(\theta_A)\right)_A$. We contend that $\varphi(\sigma)$ is an automorphism of functors. Indeed, $F_1(g) = F_1(\theta_B^{-1} \circ HG(g) \circ \theta_A)$ by the diagram of the equivalence of categories. Then

$$F_1(g) \circ \varphi(\sigma)_A = F_1\left(\theta_B^{-1} \circ HG(g) \circ \theta_A\right) F_1(\theta_A^{-1})\sigma_{G(A)}F_1(\theta_A) = F_1(\theta_B^{-1}) \circ F_1(HG(g)) \circ \sigma_{G(A)} \circ F_1(\theta_A),$$

and similarly,

$$\varphi(\sigma)_B F_1(g) = F_1(\theta_B^{-1}) \circ \sigma_{G(B)} \circ F_1(HG(g)) \circ F_1(\theta_A).$$

Using that σ is a natural transformation, we have that $\sigma_{G(B)}F_1HG(g) = F_1HG(g)\sigma_{G(A)}$, and so $F_1(g) \circ \varphi(\sigma)_A = \varphi(\sigma)_B \circ F_1(g)$ and hence $\varphi(\sigma)$ is a well-defined automorphism of the functor F_1.

It remains to show that $\varphi\psi$ and $\psi\varphi$ are identities. Let $\sigma \in \mathrm{Aut}(F)$, then

$$\psi\varphi(\sigma) = (\psi\varphi(\sigma)_X)_X = \left(F_1(\theta_{H(X)}^{-1})\sigma_{GH(X)}F_1(\theta_{H(X)})\right).$$

As σ is a natural isomorphism, it commutes with the morphism $\theta_{H(X)}$, and hence $\sigma_{GH(X)}F_1(\theta_{H(X)}) = F_1(\theta_{H(X)})\sigma_X$, and therefore $\psi\varphi(\sigma)_X = \sigma_X$, i.e., $\psi\varphi(\sigma) = \mathbf{id}_{\mathrm{Aut}(F)}$. Similarly, one can show that $\varphi\psi = \mathbf{id}_{\mathrm{Aut}(F_1)}$. This completes the proof of (b).

(a) Applying (b) to the profinite group $\pi = \varprojlim_{(A,a)\in J} \mathrm{Aut}_{\mathscr{C}}(A)$ and recall the functor H' constructed earlier which we have shown is an equivalence of categories in Theorem 3.26 which when composed with the forgetful functor F_1 yields F. Then $\pi \cong \mathrm{Aut}(F)$ and via this isomorphism we can identify H' and the previously defined $H : \mathscr{C} \to \mathrm{Aut}(F)$-**sets**. Therefore, H is an equivalence of categories.

(c) Let $F' : \mathscr{C} \to$ **Sets** be a second fundamental functor. Then we have $\varinjlim_J \mathscr{C}(A, -) \cong F$, $\varinjlim_{J'} \mathscr{C}(A, -) \cong F'$. Note that all the pairs $(A, a) \in J$ with the same A are isomorphic so we can replace J by $J_0 \subseteq J$ with exactly one pair (A, a) for each A Galois; similarly, we replace J' by $J_0' \subseteq J$ with exactly one pair (A, a) for each A Galois. Note here that the notion of Galois objects is independent of the fundamental functor.

Now given $(A, a), (B, b) \in J_0$ and $g : A \to B$ a morphism, there exists a unique $\beta \in \mathrm{Aut}_{\mathscr{C}}(B)$ such that $F(\beta)(F(g)(a)) = b$. Then $f := \beta g$ satisfies $F(f)(a) = b$, so $(A, a) \geqq_f (B, b)$ in J_0, and this happens if and only if $(A, a') \geqq_{f'} (B, b')$ in J_0' but the morphisms $f, f' : A \to B$ are not necessarily the same.

But it is true that for all $\alpha \in \mathrm{Aut}_{\mathscr{C}}(A)$, there exists a $\gamma \in \mathrm{Aut}_{\mathscr{C}}(B)$ making the following diagram commute:

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\alpha"'] & B \arrow[d, "\gamma"] \\ A \arrow[r, "f'"'] & B \end{tikzcd}$$

Now mapping $\alpha \mapsto \gamma$ we obtain a system of morphisms between the finite non-empty groups $\mathrm{Aut}_{\mathscr{C}}(A)$ giving rise to a projective sstem. Thsi limit is non-empty. This implies that we can make a simultaneous choice $(\alpha_A)_{(A,a)\in J_0}$ such that all the diagrams commute. This induces an isomorphism

$$\varinjlim_{J_0} \mathscr{C}(A, -) \cong \varinjlim_{J_0'} \mathscr{C}(A, -),$$

so that $F \cong F'$.

(d) Let $H' : \mathscr{C} \to \pi$-**sets** be an equivalence, and F' the composite of H' with the forgetful functor. Then $\pi \cong \mathrm{Aut}(F')$ by (b) and $F' \cong F$ by (c). The isomorphism between the functors F and F' induces an isomorphism $\sigma : \mathrm{Aut}(F) \to \mathrm{Aut}(F')$ by letting $\varepsilon' \in \mathrm{Aut}(F')$ correspond to $\varepsilon := \sigma\varepsilon'\sigma^{-1}$. In conclusion, $\pi \cong \mathrm{Aut}(F)$ canonically, thereby completing the proof. ■

References

[Len08] H. W. Lenstra. *Galois Theory of Schemes*. 2008.

[Sza09] Tamás Szamuely. *Galois groups and fundamental groups*, volume 117. Cambridge university press, 2009.